Computation of Euclidean minima in totally definite quaternion fields

Jean-Paul Cerri, Pierre Lezowski

COMPUTATION OF EUCLIDEAN MINIMA IN TOTALLY DEFINITE QUATERNION FIELDS

JEAN-PAUL CERRI AND PIERRE LEZOWSKI

Abstract. We describe an algorithm that allows to compute the Euclidean minimum (for the norm form) of any order of a totally definite quaternion field over a number field K of degree strictly greater than 1. Our approach is a generalization of previous work dealing with number fields. The algorithm was practically implemented when K has degree 2.

1. Introduction

If K is a number field, we denote by n its degree, by $\mathbb{Z}_K$ its ring of integers, by $\mathbb{Z}_K^\times$ its unit group, and by $N_{K/\mathbb{Q}}\colon K \to \mathbb{Q}$ the norm form. Throughout this paper F will be a *totally definite quaternion field* over a number field K. Let us recall the relevant definitions, the reader may refer to [9, 13, 15] for a complete theory. Let F be a quaternion algebra over a number field K, i.e. a 4-dimensional algebra over K with basis $(1, i, j, k)$ such that $i^2 = a$, $j^2 = b$ and $k = ij = -ji$, where a, b are non-zero elements of K. This algebra is denoted by $\left(\frac{a,b}{K}\right)$. Let $w = x + yi + zj + tk \in F$, where $x, y, z, t \in K$. We denote by $\overline{w}$ the image of w under the canonical involution of F, which is defined by $\overline{w} = x - yi - zj - tk$, and by $\mathrm{nrd}_{F/K}(w) = w\overline{w}$ its reduced norm. The algebra F is a division algebra if and only if the quadratic form $\mathrm{nrd}_{F/K}(x + yi + zj + tk) = x^2 - ay^2 - bz^2 + abt^2$ represents zero on K only trivially. In this case, we say that F is a *quaternion field*.

In addition, we will suppose that F is *totally definite*, or equivalently that every infinite place of K is ramified in F. This implies in particular that K is totally real, that a and b are totally negative and that for every $x \in F \setminus \{0\}$, $\mathrm{nrd}_{F/K}(x)$ is totally positive. Let us denote by $N\colon F \longrightarrow \mathbb{Q}_{\geq 0}$ the reduced norm map defined by $N = N_{K/\mathbb{Q}} \circ \mathrm{nrd}_{F/K}$.

Definition 1.1. Let Λ be an order of F. For any $\xi \in F$, we set

$$m_\Lambda(\xi) = \inf_{\lambda \in \Lambda} N(\xi - \lambda)$$

and we call it the *local Euclidean minimum* of Λ at ξ. We define the *Euclidean minimum* of Λ by

$$M(\Lambda) = \sup_{\xi \in F} m_\Lambda(\xi).$$

Set $F_\mathbb{R} = F \otimes_\mathbb{Q} \mathbb{R}$ and let $N_\mathbb{R}\colon F_\mathbb{R} \to \mathbb{R}_{\geq 0}$ be the extended norm corresponding to N.

Definition 1.2. Let Λ be an order of F. For any $x \in F_\mathbb{R}$, we set

$$\tilde{m}_\Lambda(x) = \inf_{\lambda \in \Lambda} N_\mathbb{R}(x - \lambda)$$

1991 *Mathematics Subject Classification.* Mathematics Subject Classification 2010: 11Y40, 11R04, 13F07.

Key words and phrases. quaternion algebras; norm-Euclidean orders; norm-Euclidean minimum; algorithmic number theory.

and we call it the *local inhomogeneous minimum* of Λ at x. We define the *inhomogeneous minimum* of Λ by

$$\widetilde{M}(\Lambda) = \sup_{x \in F_{\mathbb{R}}} \tilde{m}_{\Lambda}(x).$$

Let us notice that these suprema are well-defined positive real numbers, that $M(\Lambda) \leq \widetilde{M}(\Lambda)$ and that for every $\xi \in F$ there exists a $\lambda \in \Lambda$ such that $m_{\Lambda}(\xi) = N(\xi - \lambda)$ (see [8, 2]). Let us call (P) the following property: there exists some $\xi \in F$ such that $m_{\Lambda}(\xi) = \widetilde{M}(\Lambda)$. In particular, if (P) holds, then $M(\Lambda) = \widetilde{M}(\Lambda) \in \mathbb{Q}$. Recall that we have the following results:

- The order Λ is right-norm-Euclidean if and only if it is left-norm-Euclidean (so that we can speak of norm-Euclidean orders) and that in this case Λ is necessarily a maximal order of F;
- If $M(\Lambda) < 1$ then Λ is norm-Euclidean;
- If $M(\Lambda) > 1$ then Λ is neither right neither left-norm-Euclidean;
- If $M(\Lambda) = 1$ and if property (P) is satisfied then Λ is neither right neither left-norm-Euclidean;
- If Λ is norm-Euclidean, then every other maximal order Λ' of F is also norm-Euclidean and $M(\Lambda) = M(\Lambda')$
- If K has unit rank strictly greater than 1, i.e. $n > 2$ if K is totally real, then (P) holds.

Note that these results still hold when F is not totally definite. For more details, the reader can refer to [8, 2, 6].

A first natural question arises: what can be said when the degree of K is 1 or 2, i.e. when $K = \mathbb{Q}$ or is a real quadratic field? Do we also have $M(\Lambda) = \widetilde{M}(\Lambda)$ or does property (P) hold? We will answer to this question in Section 2, showing that the equality is always satisfied and that property (P) holds when $K = \mathbb{Q}$. Showing that it also holds when K is quadratic seems out of reach, as in the number field case, which is a famous conjecture due to Barnes and Swinnerton-Dyer.

As in the number field case (see [4, 11]), it is also natural to ask whether it is possible to use an algorithm allowing to compute $M(\Lambda) = \widetilde{M}(\Lambda)$ and to check that property (P) is satisfied, even in the conjectural case. We will see that such an algorithm is already well known when $K = \mathbb{Q}$ so that we have just to study the case where K has degree at least 2. Note also that, as in the number field case, such an algorithm might allow to determine the upper part of the so called *inhomogeneous spectrum* associated to Λ. The paper is organized as follows. In Section 2, we recall what we know when $n = 1$ and we establish some preliminary results allowing to prove $M(\Lambda) = \widetilde{M}(\Lambda)$ when $n = 2$, and that we will use later in the algorithm. In Section 3, we explain the ideas that will be used in the algorithm when $n \geq 2$. In Section 4, we describe the algorithm itself (Algorithm 2); in Section 5, we give technical details of the algorithm, and finally, in Section 6 we give the results obtained when K is quadratic, the only case that we can treat with the computers that we used.

2. Preliminary results

2.1. **The fundamental embedding.** Let $F = \left(\frac{a,b}{K}\right)$ be a totally definite quaternion field over a number field K and let Λ be an order of F. Let us denote by $\sigma_1, \ldots, \sigma_n$ the n embeddings of K into $\mathbb{R}$. Now, let us embed F into $\mathbb{R}^{4n}$ in the

following way: if $\xi = \alpha + \beta i + \gamma j + \delta k \in F$ where $\alpha, \beta, \gamma, \delta \in K$, we put

$$\Phi(\xi) = \Big(\sigma_1(\alpha), \dots, \sigma_n(\alpha), \sigma_1(\beta), \dots, \sigma_n(\beta), \sigma_1(\gamma), \dots, \sigma_n(\gamma), \sigma_1(\delta), \dots, \sigma_n(\delta)\Big),$$

and in further computations we see this vector as a column vector.
Then $\Phi(\Lambda)$ is a lattice of $\mathbb{R}^{4n}$ that will be denoted by $\mathcal{R}$. Identifying $F_{\mathbb{R}}$ with $\mathbb{R}^{4n}$, if $x \in \mathbb{R}^{4n}$ we put

$$N_{\mathbb{R}}(x) = \prod_{l=1}^{n} \mathrm{nrd}_l(x)$$

where $\mathrm{nrd}_l(x) = x_l^2 - \sigma_l(a)x_{l+n}^2 - \sigma_l(b)x_{l+2n}^2 + \sigma_l(ab)x_{l+3n}^2$. With this notation, if $\xi \in F$ and $x \in \mathbb{R}^{4n}$, we have

- $\mathrm{nrd}_l(\Phi(\xi)) = \sigma_l(\mathrm{nrd}_{F/K}(\xi))$ for every l;
- $N(\xi) = N_{\mathbb{R}}(\Phi(\xi))$;
- $\tilde{m}_\Lambda(x) = \inf_{\lambda\in\Lambda} N_{\mathbb{R}}(x - \Phi(\lambda))$;
- $m_\Lambda(\xi) = \tilde{m}_\Lambda(\Phi(\xi))$.

The multiplicative group $K \setminus \{0\}$ acts on $\mathbb{R}^{4n}$ in the following way. If $\alpha \in K \setminus \{0\}$ and $x \in \mathbb{R}^{4n}$ we put

$$\alpha \star x = (\sigma_1(\alpha)x_1, \dots, \sigma_n(\alpha)x_n, \dots, \sigma_1(\alpha)x_{3n+1}, \dots, \sigma_n(\alpha)x_{4n}).$$

Hence, if $\xi \in F$ we have $\alpha \star \Phi(\xi) = \Phi(\alpha\xi)$. Moreover, if $\nu \in \mathbb{Z}_K^\times$, then $\nu \star \mathcal{R} = \mathcal{R}$, and if $x \in \mathbb{R}^{4n}$, then $N_{\mathbb{R}}(\nu \star x) = N_{\mathbb{R}}(x)$. This implies that that for every $x \in \mathbb{R}^{4n}$ and every $\nu \in \mathbb{Z}_K^\times$, we have $\tilde{m}_\Lambda(\nu \star x) = \tilde{m}_\Lambda(x)$.

Remark 2.1. Since $\tilde{m}_\Lambda$ is $\mathcal{R}$-periodic, we have $\tilde{m}_\Lambda(\nu\star x+\Phi(\lambda)) = \tilde{m}_\Lambda(x)$ for every $(x, \nu, \lambda) \in \mathbb{R}^{4n} \times \mathbb{Z}_K^\times \times \Lambda$.

Recall that $\tilde{m}_\Lambda$ is not only $\mathcal{R}$-periodic, but also upper semi-continuous. These two properties imply that there exists an $x \in \mathbb{R}^{4n}$ such that $\widetilde{M}(\Lambda) = \tilde{m}_\Lambda(x)$. Such an x will be called *critical*.

2.2. **The case $n = 1$.** Here $K = \mathbb{Q}$, $a, b \in \mathbb{Q}_{<0}$ and we can write

$$\Lambda = \oplus_{l=1}^{4}(a_{l,1} + a_{l,2}i + a_{l,3}j + a_{l,4}k)\mathbb{Z},$$

where $a_{l,i} \in \mathbb{Q}$ for every $1 \le l, i \le 4$ and where the matrix $M = (a_{l,i})$ is invertible. We also have $F = \oplus_{l=1}^{4}(a_{l,1} + a_{l,2}i + a_{l,3}j + a_{l,4}k)\mathbb{Q} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$. With our notation, $\mathcal{R}$ is the lattice $M^t\mathbb{Z}^4 \subset \mathbb{Q}^4$ and $\Phi(F) = M^t\mathbb{Q}^4$. Let $x \in \mathbb{R}^4$ and let us put $x = M^t y$. Then $\tilde{m}_\Lambda(x) = \inf_{X\in\mathbb{Z}^4} q(M^t(y - X))$ where $q(z) = z_1^2 - az_2^2 - bz_3^2 + abz_4^2$ which is equivalent to

$$\tilde{m}_\Lambda(x) = \inf_{X\in\mathbb{Z}^4} \|SM^t(y - X)\|^2$$

where $\|\cdot\|$ is the usual Euclidean norm and $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{-a} & 0 & 0 \\ 0 & 0 & \sqrt{-b} & 0 \\ 0 & 0 & 0 & \sqrt{ab} \end{pmatrix}$. As a consequence $\widetilde{M}(\Lambda)$ is the square of the covering radius of the lattice $\mathcal{L} = SM^t\mathbb{Z}^4 \subset \mathbb{R}^4$ and if $x \in \mathbb{R}^4$ is a critical point, i.e. satisfies $\tilde{m}_\Lambda(x) = \widetilde{M}(\Lambda)$, then $\|OP\|$, where $O = (0, 0, 0, 0)$ and $P = Sx = SM^t y$, is the covering radius of $\mathcal{L}$. Let A and B be two points of $\mathcal{L}$ and let us put $A = SM^t\alpha$, $B = SM^t\beta$ where $\alpha, \beta \in \mathbb{Z}^4$. Then the mediator hyperplane of A and B is the set of $z = SM^t r$ such that $\langle SM^t(r - \frac{\alpha+\beta}{2}), SM^t(\alpha - \beta)\rangle = 0$, i.e. $\langle r - \frac{\alpha+\beta}{2}, MS^2M^t(\alpha - \beta)\rangle = 0$, where $\langle\cdot\,,\cdot\rangle$ is the usual Euclidean scalar product. Note that $\frac{\alpha+\beta}{2}, MS^2M^t(\alpha - \beta) \in \mathbb{Q}^4$. Now, the point $P = SM^t y$ belongs to 4 independent such mediator hyperplanes and the

y_i satisfy 4 independent linear equations with rational coefficients, so that $y \in \mathbb{Q}^4$. From this we deduce that $x = M^t y \in \Phi(F)$. This implies that property (P) is satisfied and that $M(\Lambda) = \widetilde{M}(\Lambda) \in \mathbb{Q}$.
Let us conclude by noting that there exist well known algorithms to compute the covering radius of $\mathcal{L}$ (see [10, 14]) and then $\widetilde{M}(\Lambda) = M(\Lambda)$, so that the case $n = 1$ is completely settled.

2.3. **Computation of $m_\Lambda(\xi)$.** From now on, we suppose that $n \geq 2$. We are interested in computing $m_\Lambda(\xi)$ where $\xi \in F$. We will rely on it for the actual computation of $M(\Lambda)$ later on.
Let $(\varepsilon_i)_{1\leq i\leq n-1}$ be a fundamental system of units of K. We denote by L the logarithmic embedding of $K \setminus \{0\}$ in $\mathbb{R}^n$ defined by

$$L(\alpha) = (\ln|\sigma_1(\alpha)|, \ldots, \ln|\sigma_n(\alpha)|).$$

We know that $L(\mathbb{Z}_K^\times)$ is a lattice of the hyperplane $\mathcal{H}$ of $\mathbb{R}^n$ defined by the equation $\sum_{1\leq i\leq n} x_i = 0$, which admits $(L(\varepsilon_i))_{1\leq i\leq n-1}$ as a $\mathbb{Z}$-basis and that the kernel of L is $\{\pm 1\}$. For $1 \leq i \leq n$ we set

$$\Gamma_i = \prod_{j=1}^{n-1} \max\Big\{|\sigma_i(\varepsilon_j)|, \frac{1}{|\sigma_i(\varepsilon_j)|}\Big\}.$$

Lemma 2.2. *Units of K have the following properties.*

(i) *Let $l \in \{1, \ldots, n\}$. There exists a $\nu \in \mathbb{Z}_K^\times$ such that $|\sigma_i(\nu)| < 1$ for every $i \neq l$.*
(ii) *If $c_1, \ldots, c_{n-1}$ are given positive real numbers, there exists a $\nu \in \mathbb{Z}_K^\times$ such that $c_i \leq \sigma_i(\nu)^2 \leq c_i\Gamma_i^2$ for all $i \in \{1, \ldots, n-1\}$.*

Proof. (i) $L(\mathbb{Z}_K^\times)$ being a lattice of $\mathcal{H}$, it is easy to see that $\mathcal{H} \cap \{x \in \mathbb{R}^n; x_l > 0 \text{ and } x_i < 0 \text{ for } i \neq l\}$, which is a nonempty open cone of $\mathcal{H}$, contains an element $L(\nu)$ of $L(\mathbb{Z}_K^\times)$.
(ii) This a consequence of [4, Lemma 3.1]. See also [5, Lemma 2.1] for a detailed proof. □

Proposition 2.3. *Let $k > 0$. Suppose that $x \in \mathbb{R}^{4n}$ and $X \in \mathcal{R}$ satisfy $N_\mathbb{R}(x-X) < k$. Then there exist an $\varepsilon \in \mathbb{Z}_K^\times$ and some $Y \in \mathcal{R}$ such that $y = \varepsilon \star x - Y$ satisfies $N_\mathbb{R}(y) < k$ and*

$$0 \leq \mathrm{nrd}_i(y) \leq \Gamma(k) \quad \textit{for every } 1 \leq i \leq n,$$

where

$$\Gamma(k) = \left(k \prod_{i=1}^{n-1} \Gamma_i^2\right)^{\frac{1}{n}}.$$

Proof. First, if $N_\mathbb{R}(x - X) = 0$ we have $\mathrm{nrd}_l(x - X) = 0$ for some index l. By Lemma 2.2 (i), there exists a $\nu \in \mathbb{Z}_K^\times$ such that $|\sigma_i(\nu)| < 1$ for every $i \neq l$. Since $\mathrm{nrd}_i(\nu^p \star x - \nu^p \star X) = \sigma_i(\nu)^{2p}\mathrm{nrd}_i(x - X)$, for p sufficiently large we have $\mathrm{nrd}_i(\nu^p \star x - \nu^p \star X) \leq \Gamma(k)$ for $i \neq l$ and $\mathrm{nrd}_l(\nu^p \star x - \nu^p \star X) = 0$. Taking $\varepsilon = \nu^p$ and $Y = \nu^p \star X$, we obtain the result announced.
Now, if $N_\mathbb{R}(x - X) \neq 0$, we apply Lemma 2.2 (ii) with $c_i = \dfrac{\Gamma(k)}{\Gamma_i^2 \mathrm{nrd}_i(x - X)}$ for $1 \leq i \leq n-1$. There exists a $\nu \in \mathbb{Z}_K^\times$ such that

$$\frac{\Gamma(k)}{\Gamma_i^2 \mathrm{nrd}_i(x - X)} \leq \sigma_i(\nu)^2 \leq \frac{\Gamma(k)}{\mathrm{nrd}_i(x - X)} \quad \text{for } 1 \leq i \leq n-1.$$

From $N_{\mathbb{R}}(\nu\star x-\nu\star X)=N_{\mathbb{R}}(x-X)=\sigma_n(\nu)^2\mathrm{nrd}_n(x-X)\prod_{i=1}^{n-1}\sigma_i(\nu)^2\mathrm{nrd}_i(x-X)$ we deduce

$$\sigma_n(\nu)^2\mathrm{nrd}_n(x-X)\leq\frac{k\prod_{i=1}^{n-1}\Gamma_i^2}{\Gamma(k)^{n-1}}=\Gamma(k).$$

Taking $\varepsilon=\nu$ and $Y=\nu\star X$ we have again the result announced. □

Now, consider the orbits of elements of $\mathbb{R}^{4n}$ under the action of $\mathbb{Z}_K^\times$. Let $x,y\in\mathbb{R}^{4n}$ and $\nu\in\mathbb{Z}_K^\times$. As $x-y\in\mathcal{R}\Rightarrow\nu\star x-\nu\star y\in\mathcal{R}$, the group $\mathbb{Z}_K^\times$ also acts on $\mathbb{R}^{4n}/\mathcal{R}$ by $(\nu,\overline{x})\mapsto\overline{\nu\star x}$, where $\overline{y}$ is the class of $y\in\mathbb{R}^{4n}$ modulo $\mathcal{R}$. Let $\mathcal{F}$ be a fundamental domain of $\mathcal{R}$. Identifying $\mathbb{R}^{4n}/\mathcal{R}$ with $\mathcal{F}$, if x_ν is the unique element of $\mathcal{F}$ congruent to $\nu\star x$ modulo $\mathcal{R}$, we set $\mathrm{Orb}(x)=\{x_\nu;\nu\in\mathbb{Z}_K^\times\}$. Remark that for all $x\in\mathbb{R}^{4n}$, if $z\in\mathrm{Orb}(x)$ we have $\tilde{m}_\Lambda(z)=\tilde{m}_\Lambda(x)$. Using this new notation, we have the following essential result.

Theorem 2.1. *There exists a finite set $\mathcal{S}\subset\mathcal{R}$ such that for every $x\in\mathbb{R}^{4n}$, we have*

$$\tilde{m}_\Lambda(x)=\inf_{z\in\mathrm{Orb}(x)}\Big(\min_{Z\in\mathcal{S}}N_{\mathbb{R}}(z-Z)\Big).$$

Proof. Let k' be any positive real number satisfying $k'>\widetilde{M}(\Lambda)$ and let $\epsilon>0$ such that $\widetilde{M}(\Lambda)+\epsilon<k'$. Let

$$\mathcal{S}'=\{t\in\mathbb{R}^{4n};\ \mathrm{nrd}_i(t)\leq\Gamma(k')\text{ for every }1\leq i\leq n\}.$$

Since for every i,

$$\mathrm{nrd}_i(t)=t_i^2-\sigma_i(a)t_{i+n}^2-\sigma_i(b)t_{i+2n}^2+\sigma_i(ab)t_{i+3n}^2,$$

where $\sigma_i(a),\sigma_i(b)<0$, we see that $\mathcal{S}'$ is a bounded subset of $\mathbb{R}^{4n}$. Now, let us put

$$\mathcal{S}=(\mathcal{F}+\mathcal{S}')\cap\mathcal{R}.$$

As $\mathcal{S}'+\mathcal{F}$ is also bounded, the set $\mathcal{S}$ is a finite subset of $\mathcal{R}$. Let $x\in\mathbb{R}^{4n}$. There exists some $X\in\mathcal{R}$ such that $N_{\mathbb{R}}(x-X)<\tilde{m}_\Lambda(x)+\epsilon\leq\widetilde{M}(\Lambda)+\epsilon<k'$. Applying Proposition 2.3 with $k=\tilde{m}_\Lambda(x)+\epsilon$, we see that there exists a $\nu\in\mathbb{Z}_K^\times$ and some $Y\in\mathcal{R}$ such that, if $y=\nu\star x-Y$, then $N_{\mathbb{R}}(y)<\tilde{m}_\Lambda(x)+\epsilon<k'$ and $\mathrm{nrd}_i(y)\leq\Gamma(\tilde{m}_\Lambda(x)+\epsilon)\leq\Gamma(k')$ (because Γ is an increasing function). Let $z\in\mathcal{F}$ such that $z-y\in\mathcal{R}$. Then, $z\in\mathrm{Orb}(x)$ and $y=z-Z$, where $Z\in\mathcal{S}$ and $N_{\mathbb{R}}(z-Z)<\tilde{m}_\Lambda(x)+\epsilon$. Since this is true for any $\epsilon>0$ we have

$$\tilde{m}_\Lambda(x)\geq\inf_{z\in\mathrm{Orb}(x)}\Big(\min_{Z\in\mathcal{S}}N_{\mathbb{R}}(z-Z)\Big).$$

On the other hand, for every $z\in\mathrm{Orb}(x)$ and any $Z\in\mathcal{R}$, we have $\tilde{m}_\Lambda(x)=\tilde{m}_\Lambda(z)\leq N_{\mathbb{R}}(z-Z)$, which leads to the equality. □

Remark 2.4. This result shows that if $x\in\Phi(F)$, we can compute $\tilde{m}_\Lambda(x)$ in a finite number of steps. In fact, $\mathrm{Orb}(x)$ is finite if and only $x\in\Phi(F)$. Indeed, if $x\in\Phi(F)$ we can write $x=X/d$ where $X\in\mathcal{R}$ and $d\in\mathbb{Z}_{>}0$, and $\mathrm{Orb}(x)$ can be identified with a subset of $\mathcal{R}/d\mathcal{R}$ which is finite. Conversely, if $\mathrm{Orb}(x)$ is finite and if ν is a nontorsion unit of K, considering the sequence $(x_{\nu^p})_{p\geq0}$, we see that there exists $k>l\geq0$ such that $x_{\nu^k}=x_{\nu^l}$. This implies that there exists an $X=\Phi(\lambda)\in\mathcal{R}$, with $\lambda\in\Lambda$, such that $(\nu^k-\nu^l)\star x=X$ which implies $x=\Phi(\lambda/(\nu^k-\nu^l))\in\Phi(F)$. As in the number field case, this allows to establish an algorithm to compute $\tilde{m}_\Lambda(x)$. We could use the formula for $\mathcal{S}$ in the proof of Theorem 2.1 but we do not know $\widetilde{M}(\Lambda)$, so we cannot compute $\mathcal{S}$. However, we can proceed as follows. Let us take some $k'>0$ and set $\mathcal{S}_{k'}=\mathcal{S}$ as defined in the previous proof. Let us put

$$\mathcal{M}_{k'}=\min_{z\in\mathrm{Orb}(x)}\left(\min_{Z\in\mathcal{S}_{k'}}\Big(N_{\mathbb{R}}(z-Z)\Big)\right).\tag{1}$$

Then

$$\mathcal{M}_{k'} \leq k' \;\Rightarrow\; \tilde{m}_\Lambda(x) = \mathcal{M}_{k'}.$$

Of course, $\tilde{m}_\Lambda(x) \leq \mathcal{M}_{k'}$. Suppose that $\tilde{m}_\Lambda(x) < \mathcal{M}_{k'}$ so that there exists some $X \in \mathcal{R}$ such that $N_{\mathbb{R}}(x - X) < \mathcal{M}_{k'}$. Then by Proposition 2.3 there exists a $\nu \in \mathbb{Z}_K^\times$ and some $Y \in \mathcal{R}$ such that if $y = \nu \star x - Y$, then $N_{\mathbb{R}}(y) < \mathcal{M}_{k'}$ and $\mathrm{nrd}_i(y) \leq \Gamma(\mathcal{M}_{k'}) \leq \Gamma(k')$ for every i. This contradicts the definition of $\mathcal{M}_{k'}$. Finally, we have the following algorithm to compute $\tilde{m}_\Lambda(x)$.

Algorithm 1: Computation of $\tilde{m}_\Lambda(x)$ when $x \in \Phi(F)$

Input: $x \in \Phi(F)$.
Output: $\tilde{m}_\Lambda(x)$.
1 Computation of $\mathrm{Orb}(x)$.
2 Computation of $k'' = \mathcal{M}_{k'}$ for a $k' > 0$.
3 **if** $k'' \leq k'$ **then**
4 $\tilde{m}_\Lambda(x) = k''$
5 **else**
6 Computation of $k = \mathcal{M}_{k''}$.
7 $\tilde{m}_\Lambda(x) = k$.

The correctness of the algorithm follows from the fact that $k' \longmapsto \mathcal{M}_{k'}$ is a decreasing function: if $k'' > k'$ then $M_{k''} \leq M_{k'} = k''$ and $\tilde{m}_\Lambda(x) = M_{k''}$.

2.4. **The case $n = 2$.** Here we use Theorem 2.1 to show that when $n = 2$, as in every other case, we have $M(\Lambda) = \widetilde{M}(\Lambda)$.

Theorem 2.2. *If $n = 2$, then $M(\Lambda) = \widetilde{M}(\Lambda)$.*

Proof. We follow the idea of the proof given by Barnes and Swinnerton-Dyer in the real quadratic number field case [1]. Let $K = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is a squarefree integer. Denote by σ the nontrivial embedding of K into $\mathbb{R}$, i.e. the $\mathbb{Q}$-automorphism of K such that $\sigma(\sqrt{d}) = -\sqrt{d}$. Let ν be a fundamental unit of K. We can suppose $\nu > 1$ so that $|\sigma(\nu)| < 1$. Let $\epsilon > 0$. Keep the notation of the proof of Theorem 2.1. The map $N_{\mathbb{R}}$ being continuous, let $\epsilon' > 0$ such that for every $x, y \in \mathcal{F} + \mathcal{S} + \{z \in \mathbb{R}^{4n};\ |z_i| < 1 \text{ for all } i\}$, which is a bounded set, if $|x_i - y_i| < \epsilon'$ for every i, then $|N_{\mathbb{R}}(x) - N_{\mathbb{R}}(y)| < \epsilon$. Choose $\epsilon' < 1$. Let $x \in \mathbb{R}^8$ such that $\tilde{m}_\Lambda(x) = \widetilde{M}(\Lambda)$. If $x \in \Phi(F)$ we are done, so that we can suppose $x \notin \Phi(F)$. The set $\{x_{\nu^p};\ p \geq 0\} \subset \mathcal{F}$ is infinite and bounded , and there exist $n_2 > n_1 \geq 0$ such that for every i, $|(x_{\nu^{n_2}})_i - (x_{\nu^{n_1}})_i| < \epsilon'/2$. Without loss of generality we can suppose $\nu^{n_2 - n_1} > 2$. We have $\nu^{n_2-n_1} \star x_{\nu^{n_1}} = x_{\nu^{n_2}} + X$ where $X \in \mathcal{R}$. Let us put $X = \Phi(\lambda)$ with $\lambda \in \Lambda$. Set

$$\xi = \frac{\lambda}{\nu^{n_2-n_1} - 1} \in F \quad \text{and} \quad \alpha = \Phi(\xi) \in \Phi(F).$$

Since $\nu^{n_2-n_1} \star \alpha = \alpha \bmod \mathcal{R}$, we have

$$\mathrm{Orb}(\alpha) = \bigcup_{k=0}^{n_2-n_1-1} \{\alpha_{\nu^k}, \alpha_{-\nu^k}\} \subset \mathcal{F}.$$

It is easy to see that

$$\alpha_i = \begin{cases} (x_{\nu^{n_1}})_i + \dfrac{(x_{\nu^{n_1}})_i - (x_{\nu^{n_2}})_i}{\nu^{n_2-n_1} - 1} & \text{for } i \text{ odd}, \\ (x_{\nu^{n_1}})_i + \dfrac{(x_{\nu^{n_1}})_i - (x_{\nu^{n_2}})_i}{\sigma(\nu)^{n_2-n_1} - 1} & \text{for } i \text{ even}. \end{cases}$$

Since $|(x_{\nu^{n_1}})_i - (x_{\nu^{n_2}})_i| < \epsilon'/2$ and $\nu^{n_2-n_1} > 2$, this implies that

$$|\alpha_i - (x_{\nu^{n_1}})_i| < \frac{\epsilon'}{\nu^{n_2-n_1}} \quad \text{for } i \text{ odd},$$
$$\text{and } |\alpha_i - (x_{\nu^{n_1}})_i| < \epsilon' \quad \text{for } i \text{ even}.$$

Consequently for every $0 \leq k < n_2 - n_1$, we have

$$|(\nu^k \star \alpha)_i - (\nu^k \star x_{\nu^{n_1}})_i| < \epsilon' \quad \text{for all } i. \tag{2}$$

Now, for every $0 \leq k < n_2 - n_1$, $\nu^k \star \alpha = \alpha_{\nu^k} + X_k$ where $X_k \in \mathcal{R}$. Let $X \in \mathcal{S}$. Then for every i, we have

$$|(\alpha_{\nu^k} - X)_i - (\nu^k \star x_{\nu^{n_1}} - X_k - X)_i| < \epsilon'.$$

But $\alpha_{\nu^k} - X \in \mathcal{F} + \mathcal{S}$ and since $\epsilon' < 1$, we have $\nu^k \star x_{\nu^{n_1}} - X_k - X \in \mathcal{F} + \mathcal{S} + \{z \in \mathbb{R}^{4n};\ |z_i| < 1 \text{ for all } i\}$. By choice of ϵ' this implies that for every $0 \leq k < n_2 - n_1$,

$$|N_{\mathbb{R}}(\alpha_{\nu^k} - X) - N_{\mathbb{R}}(\nu^k \star x_{\nu^{n_1}} - X_k - X)| < \epsilon. \tag{3}$$

Now inequality (2) shows that for every $0 \leq k < n_2 - n_1$,

$$|(-\nu^k \star \alpha)_i - (-\nu^k \star x_{\nu^{n_1}})_i| < \epsilon' \quad \text{for all } i.$$

Putting $-\nu^k \star \alpha = \alpha_{-\nu^k} + Y_k$ where $Y_k \in \mathcal{R}$ for $0 \leq k < n_2 - n_1$, we obtain in the same way that for every $x \in \mathcal{S}$ and every $0 \leq k < n_2 - n_1$,

$$|N_{\mathbb{R}}(\alpha_{-\nu^k} - X) - N_{\mathbb{R}}(-\nu^k \star x_{\nu^{n_1}} - Y_k - X)| < \epsilon. \tag{4}$$

Thus, by (3) and (4), for every $y \in \mathrm{Orb}(\alpha)$ and every $X \in \mathcal{S}$,

$$N_{\mathbb{R}}(y - X) > N_{\mathbb{R}}(z - Z) - \epsilon$$

for some $z \in \mathrm{Orb}(x_{\nu^{n_1}})$ and $Z \in \mathcal{R}$. We deduce from Theorem 2.1 that

$$\tilde{m}_\Lambda(\alpha) > \tilde{m}_\Lambda(x_{\nu^{n_1}}) - \epsilon = \tilde{m}_\Lambda(x) - \epsilon = \widetilde{M}(\Lambda) - \epsilon.$$

Since for every $\epsilon > 0$, there exists some $\alpha \in \Phi(F)$ such that $\tilde{m}_\Lambda(\alpha) > \widetilde{M}(\Lambda) - \epsilon$, we have necessarily $M(\Lambda) = \widetilde{M}(\Lambda)$. □

Remark 2.5. The second part of our proof does not follow [1] because the third "equation" of [1, p. 313] is incorrect.

Corollary 2.6. *In all cases, we have* $M(\Lambda) = \widetilde{M}(\Lambda)$.

Proof. By [2], the equality holds when $n > 2$, and by Subsection 2.2, it also holds when $n = 1$. Of course, in both cases we have a better result since property (P) holds. □

3. Theoretic argumentation

3.1. **Overview of the strategy.** Now, it is time to set out the ideas which are behind the algorithm used to compute $M(\Lambda) = \widetilde{M}(\Lambda)$ when $n \geq 2$. The strategy is the same as in the number field case.

To simplify things we assume that we have an idea of the exact value of $M(\Lambda)$. We shall see later how one can find a good candidate for the Euclidean minimum. From now on, we denote by k our guess of $M(\Lambda)$.

In fact, instead of proving the equality $M(\Lambda) = k$, we shall establish the stronger and more precise result:

$$\widetilde{M}(\Lambda) \leq k \text{ and there exists a } \xi \in F \text{ such that } m_\Lambda(\xi) = k.$$

It will clearly follow that $M(\Lambda) = \widetilde{M}(\Lambda) = k$. Moreover, we shall try to find all the critical points which belong to F.

Since $\tilde{m}_\Lambda$ is $\mathcal{R}$-periodic, it is sufficient to work on a fundamental domain $\mathcal{F}$ of $\mathcal{R}$, i.e. to prove that for all $x \in \mathcal{F}$, $\tilde{m}_\Lambda(x) \leq k$, and to find all the $\xi \in F$ such that $\Phi(\xi) \in \mathcal{F}$ and $m_\Lambda(\xi) = k$ (every solution to $m_\Lambda(\xi) = k$ will be of this form modulo Λ).

Let k' be a positive number smaller than k. In practice one takes $k' = k - \epsilon$ where ϵ is a small positive number. Let us consider a finite family of elements of $\mathcal{R}$, say $\mathcal{X}$, and the regions of $\mathbb{R}^{4n}$ centered in the X of $\mathcal{X}$ and defined by the inequations $N_{\mathbb{R}}(x - X) \leq k'$. Every element x of the subset H of $\mathcal{F}$ covered by these regions satisfies $\tilde{m}_\Lambda(x) \leq k' < k$, and since k' is supposed smaller than $\widetilde{M}(\Lambda)$, "holes" appear in the covering of $\mathcal{F}$ by these regions. These holes contain the potentially critical points of $\mathcal{F}$.

The main idea is then to analyze the action of the unit group $\mathbb{Z}_K^\times$ on uncovered subsets of $\mathcal{F}$, in the following way. Let $\mathcal{T}$ be a hole of $\mathcal{F}$, and ε a non-torsion unit of K ($\varepsilon \neq \pm 1$). We look at the possible intersections of $\varepsilon \star \mathcal{T}$ with holes of $\mathcal{F}$ modulo $\mathcal{R}$. If $\varepsilon \star \mathcal{T}$ does not intersect any hole of $\mathcal{F}$ modulo $\mathcal{R}$, we know by Remark 2.1 that for every x of $\mathcal{T}$, we have $\tilde{m}_\Lambda(x) \leq k'$, so that $\mathcal{T}$ can be eliminated as a subset of $\mathcal{F}$ potentially containing a critical point. The interesting case is when the intersection is nonempty.

Remark 3.1. Here we have expressed things in terms of holes. In what follows, we consider "easy" regions larger than holes. For instance, in the algorithm, holes are replaced by regions composed of small parallelotopes. All what we need is to have a partition of $\mathcal{F}$ in a covered region and in regions potentially containing critical points. Then we check that these regions have an exploitable behaviour under the action of $\mathbb{Z}_K^\times$.

3.2. **Theoretic arguments.** As in the previous subsection, we consider $k' > 0$ and and a subset $\mathcal{H}$ of $\mathbb{R}^{4n}$ which satisfies $\tilde{m}_\Lambda(x) \leq k'$ for all $x \in \mathcal{H}$. We consider also a unit $\varepsilon \neq \pm 1$.

3.2.1. *The cyclic case.* Let us first study the cyclic situation.

Theorem 3.1. *Let $\mathcal{T}_0, \ldots, \mathcal{T}_{j-1}$ be bounded subsets of $\mathbb{R}^{4n}$ ($j \geq 1$). Assume that for all l there is an $\Upsilon_l \in \Lambda$ such that*

$$(\varepsilon \star \mathcal{T}_l - \Phi(\Upsilon_l)) \setminus \mathcal{H} \subset \mathcal{T}_{l+1}, \tag{5}$$

where the indices in $\mathcal{T}_r$ are to be read modulo j. Assume also that there is an x in $\mathcal{T}_0$ which satisfies $\tilde{m}_\Lambda(x) > k'$ and define $\Omega \in \Lambda$ by

$$\Omega = \varepsilon^{j-1}\Upsilon_0 + \varepsilon^{j-2}\Upsilon_1 + \ldots + \varepsilon\Upsilon_{j-2} + \Upsilon_{j-1}.$$

Consider the sequence defined by $y_0 = x$ and $y_{p+1} = \varepsilon^j \star y_p - \Phi(\Omega)$ for all $p \geq 0$. Then, if we put

$$\xi = \frac{\Omega}{\varepsilon^j - 1} \in F \quad \text{and} \quad t = \Phi(\xi),$$

we have

i) *For all $i \in \{1, \ldots, n\}$ such that $|\sigma_i(\varepsilon)| > 1$ and for all $p \geq 0$ and all $k \in \{0, 1, 2, 3\}$, $(y_p)_{i+kn} = t_{i+kn}$.*
ii) *The sequence $(y_p)_{p \geq 0}$ converges to t.*
iii) *$k' < \tilde{m}_\Lambda(x) \leq \tilde{m}_\Lambda(t)$.*
iv) *If $x \in \Phi(F)$ then $x = t$.*

Proof. Put $\mathcal{H}' = \{x \in \mathbb{R}^{4n};\ \tilde{m}_\Lambda(x) \leq k'\}$ so that $\mathcal{H} \subset \mathcal{H}'$. First of all, let us prove that

$$\big(\varepsilon^j \star \mathcal{T}_0 - \Phi(\Omega)\big) \setminus \mathcal{H}' \subset \mathcal{T}_0. \tag{6}$$

Put $z = \varepsilon^j \star z_0 - \Phi(\Omega)$ where $z_0 \in \mathcal{T}_0$ and suppose $z \notin \mathcal{H}'$. Let us define z_1, $z_2, \ldots, z_j$ by the induction formula $z_{p+1} = \varepsilon \star z_p - \Phi(\Upsilon_p)$ for $0 \leq p < j$.
It is easy to see that we have $z_j = z$. By Remark 2.1 we can write

$$\tilde{m}_\Lambda(z) = \tilde{m}_\Lambda(z_j) = \tilde{m}_\Lambda(z_{j-1}) = \ldots = \tilde{m}_\Lambda(z_0) > k'.$$

Thus for all $p \in \{0, \ldots, j\}$ we have $z_p \notin \mathcal{H}'$, which implies $z_p \notin \mathcal{H}$, and by successive applications of (5) we get $z_p \in \mathcal{T}_p$ for all $p \in \{0, \ldots, j-1\}$, and finally $z = z_j \in \mathcal{T}_0$, so that we have (6).

Now, consider the sequence $(y_p)_{p\geq 0}$. By Remark 2.1 we see by induction that for all $p \geq 0$

$$\tilde{m}_\Lambda(y_p) = \tilde{m}_\Lambda(x) > k' \tag{7}$$

so that for all $p \geq 0$, $y_p \notin \mathcal{H}'$. Then, as $y_0 = x \in \mathcal{T}_0$, using (6) we easily establish by induction that $y_p \in \mathcal{T}_0$ for all $p \geq 0$. Thus, as $\mathcal{T}_0$ was assumed to be bounded, the sequence $(y_p - t)_{p\geq 0}$ is bounded.

But, by the definition of t and the induction formula which defines $(y_p)_{p\geq 0}$, we have $y_p - t = \varepsilon^{jp} \star (x - t)$ for all $p \geq 0$, so that

$$|(y_p)_i - t_i| = |\sigma_{i \bmod n}(\varepsilon)|^{jp} \, |x_i - t_i| \text{ for all } i \in \{1, 2, \ldots, 4n\} \text{ and for all } p \geq 0. \tag{8}$$

Let $i \in \{1, \ldots, n\}$.
If $|\sigma_i(\varepsilon)| > 1$, since the sequence $(|(y_p)_{i+kn} - t_{i+kn}|)_{p\geq 0}$ is bounded for every $k \in \{0, 1, 2, 3\}$, we must have $x_{i+kn} - t_{i+kn} = 0$, and then by (8) we obtain

$$(y_p)_{i+kn} = t_{i+kn} \text{ for all } k \in \{0, 1, 2, 3\} \text{ and for all } p \geq 0. \tag{9}$$

This is i).

Moreover if $|\sigma_i(\varepsilon)| < 1$, then (8) shows that

$$\lim_{p\to+\infty} (y_p)_{i+kn} = t_{i+kn} \text{ for all } k \in \{0, 1, 2, 3\}. \tag{10}$$

Since $|\sigma_i(\varepsilon)| \neq 1$ (otherwise $\varepsilon = \pm 1$, which is excluded by hypothesis), (9) and (10) yield

$$\lim_{p\to+\infty} y_p = t.$$

This is ii). Finally, since $\tilde{m}_\Lambda$ is upper semi-continuous, by (7), we obtain:

$$k' < \tilde{m}_\Lambda(x) = \limsup_{p\to+\infty} \tilde{m}_\Lambda(y_p) \leq \tilde{m}_\Lambda(t),$$

which gives iii).

Now, assume that $x \in \Phi(F)$. Since we cannot have $|\sigma_i(\varepsilon)| \leq 1$ for every i, there exists an $i \in \{1, \ldots, n\}$ such that $|\sigma_i(\varepsilon)| > 1$, and by i) (with $p = 0$) we have

$$x_{i+kn} = t_{i+kn} \text{ for every } k \in \{0, 1, 2, 3\}. \tag{11}$$

But x and t are both in $\Phi(F)$, and if we write $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, $t = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$ with $\alpha_j, \beta_j \in K$ for every j, by (11) we have $\sigma_i(\alpha_j) = \sigma_i(\beta_j)$ for every j. By injectivity of σ_i, this leads to $\alpha_j = \beta_j$ for every j, so that $x = t$. □

Remark 3.2. Obviously the same property holds for $\mathcal{T}_1$, $\mathcal{T}_2, \ldots, \mathcal{T}_{j-1}$, the single difference is the formula for Ω, in which indices must be trivially permuted. More precisely, for $r \in \{0, \ldots, j-1\}$, if we put $t_r = \Phi(\xi_r)$ with

$$\xi_r = \frac{\Omega_r}{\varepsilon^j - 1},$$
$$\text{and } \Omega_r = \varepsilon^{j-1}\Upsilon_r + \varepsilon^{j-2}\Upsilon_{r+1} + \ldots + \Upsilon_{r+j-1},$$

where the indices are still to be read modulo j, we have the same property as in Theorem 3.1 for $\mathcal{T}_r$ (with t_r instead of t). Moreover $t_0 = t$ and we have the cyclic law:

$$t_{r+1} = \Phi(\varepsilon) \cdot t_r - \Phi(\Upsilon_r)$$

for all $r \in \{0, \ldots, j-1\}$. In particular, all the t_r are in $\mathrm{Orb}(t)$.

3.2.2. *Generalization.* Even if Theorem 3.1 allows one to treat some situations, it is not sufficient, in the form seen above, to cover all the cases that one meets in practice. A generalization of the previous situation is the following one.

Let $\mathcal{T}_i$ $(0 \leq i \leq s-1)$ be distinct bounded sets of $\mathbb{R}^{4n}$, and $T = \{\mathcal{T}_0, \ldots, \mathcal{T}_{s-1}\}$. Assume that for all $\mathcal{T}_i$ in T there exists an $X_i \in \mathcal{R}$ and s_i integers $n_{i,1}, \ldots, n_{i,s_i}$ $(s_i > 0)$ such that

$$(\varepsilon \star \mathcal{T}_i - X_i) \setminus \mathcal{H} \subset \bigcup_{1 \leq k \leq s_i} \mathcal{T}_{n_{i,k}}. \tag{12}$$

To simplify notation we shall consider the $\mathcal{T}_i$ as the vertices of a directed graph (from now on digraph) G and represent (12) by s_i directed edges (from now on arcs) whose tail is $\mathcal{T}_i$ and whose respective heads are the $\mathcal{T}_{n_{i,k}}$ $(1 \leq k \leq s_i)$. Of course, such an arc can be a loop.
We shall write $\mathcal{T}_i \to \mathcal{T}_{n_{i,k}}$ (X_i) or $\mathcal{T}_i \to \mathcal{T}_{n_{i,k}}$, if it is not necessary to precise X_i.

Example 3.3. Theorem 3.1 corresponds to the digraph

$$G_1 \colon \mathcal{T}_0 \to \mathcal{T}_1\ (\Phi(\Upsilon_0)) \to \ldots \to \mathcal{T}_{j-1}\ (\Phi(\Upsilon_{j-2})) \to \mathcal{T}_0\ (\Phi(\Upsilon_{j-1})).$$

To describe paths of G we shall use the notation $\mathcal{T}'_1 \to \mathcal{T}'_2 \to \ldots \to \mathcal{T}'_k$.

The digraph G has the following properties: if $\mathcal{T}$ and $\mathcal{T}'$ are vertices of G, there is at most one arc whose tail is $\mathcal{T}$ and whose head is $\mathcal{T}'$, and every vertex of G has a positive outvalency. Obviously the last property implies that G contains circular paths (or circuits). Consequently, the set $\mathcal{C}$ of simple circuits of G (paths of the form $\mathcal{T}'_0 \to \ldots \to \mathcal{T}'_k \to \mathcal{T}'_0$, where $k \geq 0$ and all the $\mathcal{T}'_i$ are distinct) is *nonempty* (take a circuit of minimal length) and is *finite* (their length cannot exceed s). Each element c of $\mathcal{C}$ of length j is of the form of the circular path met in Theorem 3.1 (and seen above in G_1), $\mathcal{T}'_0 \to \mathcal{T}'_1(X'_0) \ldots \to \mathcal{T}'_{j-1}(X'_{j-2}) \to \mathcal{T}'_0(X'_{j-1})$ with $X'_i = \Phi(\Upsilon_i)$. It defines, in a unique way, j points of $\Phi(F)$, $t_0, \ldots, t_{j-1}$ by the formulae of Remark 3.2.

In this context, we say that $t_0, \ldots, t_{j-1}$ are *associated* to c (implicitly t_i corresponds to $\mathcal{T}'_i$). The t_i are in the same orbit modulo $\mathcal{R}$ and satisfy $\tilde{m}_\Lambda(t_0) = \ldots = \tilde{m}_\Lambda(t_{j-1})$.
Let us denote this rational number by $m_\Lambda(c)$ and put

$$m_\Lambda(G) = \max_{c \in \mathcal{C}} m_\Lambda(c).$$

Moreover, let us denote by $\mathcal{E}$ the set of all points of $\Phi(F)$ associated to the elements of $\mathcal{C}$. The set $\mathcal{E}$ is *finite* and we also have

$$m_\Lambda(G) = \max_{t \in \mathcal{E}} \tilde{m}_\Lambda(t).$$

Finally let us put

$$\mathcal{E}' = \{t \in \mathcal{E} \text{ such that } \tilde{m}_\Lambda(t) = m_\Lambda(G)\}.$$

An *infinite path* of G is an infinite sequence of arcs of G, $(A_i)_{i \geq 0}$ such that the head of A_i is the tail of A_{i+1}. If A_i is defined by $\mathcal{T}'_i \to \mathcal{T}'_{i+1}$, we shall denote the path by $(\mathcal{T}'_i)_{i \geq 0}$. Such a path is not simple, but can have a periodicity property. An infinite path $(\mathcal{T}'_i)_{i \geq 0}$ is said to be *ultimately periodic* if there exist integers $r \geq 0$ and $p \geq 1$ such that

$$\text{for all } i \geq r,\ \mathcal{T}'_{i+p} = \mathcal{T}'_i. \tag{13}$$

Let $(\mathcal{T}'_i)_{i\geq 0}$ be an ultimately periodic infinite path. Let $\mathcal{P}$ be the set of $p \geq 1$ such that there exists an r which satisfies (13). Then $\mathcal{P}$ is nonempty and we can define

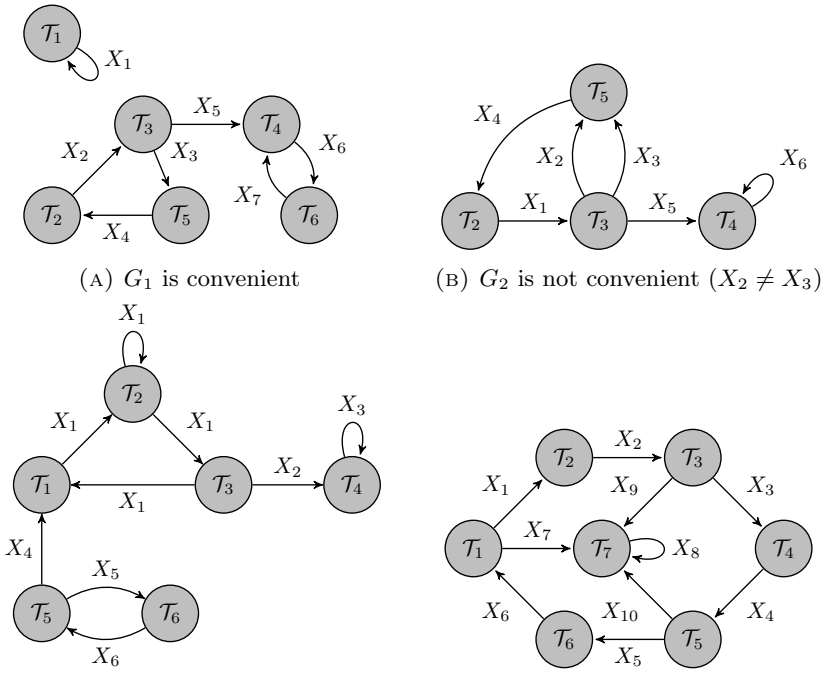
$$\rho = \min \mathcal{P} \geq 1.$$

Then there exists an r_ρ such that $\forall i \geq r_\rho$, $\mathcal{T}'_{i+\rho} = \mathcal{T}'_i$. The integer ρ will be called the *period length* of $(\mathcal{T}'_i)_{i\geq 0}$ and every circuit $\mathcal{T}'_i \to \ldots \to \mathcal{T}'_{i+\rho}$, where $i \geq r_\rho$, will be called a *period* of $(\mathcal{T}'_i)_{i\geq 0}$

Definition 3.4. We shall say that G is *convenient* if every infinite path of G is ultimately periodic.

Convenient digraphs have the following properties. Assume that G is convenient. Then every circuit is a power of a simple circuit. It can be shown that this condition implies that G is convenient. Another characterisation of convenient digraphs could be the following one: two distinct simple circuits have no common vertex. Assume that G is convenient and let $P = (\mathcal{T}'_i)_{i\geq 0}$ be an infinite path of G. Then, every period of P is a simple circuit (see [4] for more details).

Example 3.5. G_1 is convenient. Figure 1 gives examples of convenient and not convenient digraphs.



(A) G_1 is convenient (B) G_2 is not convenient ($X_2 \neq X_3$)

(C) G_3 is not convenient (D) G_4 is convenient

FIGURE 1. Some digraphs.

Now, we can establish the theorem which will allow us to treat (almost) all the situations.

Theorem 3.2. *Assume that G is convenient and that there exist a $\mathcal{T} \in T$ and an $x \in \mathcal{T}$ such that $\tilde{m}_\Lambda(x) > k'$. Then*

i) $k' < \tilde{m}_\Lambda(x) \leq m_\Lambda(G)$.
ii) *If $x \in \Phi(F)$, there exists a $t \in \mathcal{E}$ such that $x \equiv t \bmod \mathcal{R}$.*
iii) *If $x \in \Phi(F)$ is critical, there exists a $t \in \mathcal{E}'$ such that $x \equiv t \bmod \mathcal{R}$.*

Proof. The proof is exactly the same as the proof of Theorem 4.5 of [4] with some changes of notation. Let us rephrase it. Put $x_0 = x$ and $\mathcal{T}'_0 = \mathcal{T}$. By (12) we know that there exists $X'_0 \in \mathcal{R}$ and s'_0 elements of T, denoted by $\mathcal{T}_{n'_{0,k}}$ $(1 \leq k \leq s'_0)$ such that

$$(\varepsilon \star \mathcal{T}'_0 - X'_0) \setminus \mathcal{H} \subset \bigcup_{1 \leq k \leq s'_0} \mathcal{T}_{n'_{0,k}}.$$

Set $x_1 = \varepsilon \star x_0 - X'_0$. Since $\tilde{m}_\Lambda(x_1) = \tilde{m}_\Lambda(x_0) > k'$, we have

$$x_1 \in (\varepsilon \star \mathcal{T}'_0 - X'_0) \setminus \mathcal{H},$$

and necessarily, there is an $i \in \{1, \ldots, s'_0\}$ such that $x_1 \in \mathcal{T}_{n'_{0,i}}$. We put $\mathcal{T}'_1 = \mathcal{T}'_{n'_{0,i}}$, and we continue with $x_2 = \varepsilon \star x_1 - X'_1$ where X'_1 is the element of $\mathcal{R}$ associated to $\mathcal{T}'_1$ by (12). We see that we can construct by induction a sequence $(x_i)_{i \geq 0}$ and an infinite path $(\mathcal{T}'_i)_{i \geq 0}$ which satisfy: $x_0 = x$, for all $i \geq 0$, $x_{i+1} = \varepsilon \star x_i - X'_i$ where $X'_i \in \mathcal{R}$ and

$$\text{for all } i \geq 0,\ x_i \in \mathcal{T}'_i. \tag{14}$$

Moreover, by Remark 2.1, we have $\tilde{m}_\Lambda(x_i) = \tilde{m}_\Lambda(x) > k'$ for all i.
G being convenient, the infinite path $(\mathcal{T}'_i)_{i \geq 0}$ is ultimately periodic. We denote its period length ρ and we consider one of its periods c, described by $\mathcal{T}'_r \to \ldots \to \mathcal{T}'_{r+\rho} = \mathcal{T}'_r$, which is a simple circuit.
Define $\mathcal{T}''_s = \{x_{r+s+i\rho};\ i \in \mathbb{N}\}$, for $0 \leq s \leq \rho - 1$.
By (14) we have $\forall s \in \{0, \ldots, \rho - 1\}$, $\mathcal{T}''_s \subset \mathcal{T}'_{r+s}$. This implies that the $\mathcal{T}''_s$ are bounded. Moreover, by construction, for all s there exists $\Upsilon_s \in \Lambda$ (in fact $\Phi^{-1}(X'_{r+s})$) such that

$$\varepsilon \star \mathcal{T}''_s - \Phi(\Upsilon_s) \setminus \mathcal{H} = \varepsilon \star \mathcal{T}''_s - \Phi(\Upsilon_s) \subset \mathcal{T}''_{s+1}$$

where the indices are to be read modulo ρ. Putting $y = x_r \in \mathcal{T}''_0$ which satisfies $\tilde{m}_\Lambda(y) > k'$, we see that we are exactly under the hypotheses of Theorem 3.1 (with y instead of x, $\mathcal{T}''_i$ instead of $\mathcal{T}_i$ and ρ instead of j). This theorem defines ρ rational points t_i associated to the simple circuit c.
By definition of $m_\Lambda(c)$, and by Theorem 3.1.iii), we obtain

$$k' < \tilde{m}_\Lambda(x) = \tilde{m}_\Lambda(x_r) \leq m_\Lambda(c),$$

and by definition of $m_\Lambda(G)$ we have i).

Assume now that $x \in \Phi(F)$ so that, by induction, $x_r \in \Phi(F)$. By Theorem 3.1.iv) we have $x_r = t_0$, and thus $x_r - t_0 \in \mathcal{R}$. By the induction formula of the definition of (x_i) and the formulae of Remark 3.2, we see that

$$\text{for all } k \in \{0, \ldots, r\},\ \varepsilon \star (x_{r-k} - t_{-k}) \in \mathcal{R},$$

where the index in t_{-k} is taken modulo ρ. Finally, $x = x_0 \equiv t_{-r} \bmod \mathcal{R}$ which is an element of $\mathcal{E}$ by definition of $\mathcal{E}$. This proves ii).

Assume now that x is critical so that we have $\tilde{m}_\Lambda(x) = \widetilde{M}(\Lambda)$. From the definitions, we can write $\tilde{m}_\Lambda(x) \geq m_\Lambda(G)$ and by i) we obtain $\tilde{m}_\Lambda(x) = m_\Lambda(G)$ so that $\tilde{m}_\Lambda(t_{-r}) = m_\Lambda(G)$. Since $t_{-r} \in \mathcal{E}$, we find $t_{-r} \in \mathcal{E}'$. This proves iii). □

4. The algorithm, theoretic aspect

4.1. **General strategy.** Let Λ be an order of F. Since Λ is a torsion-free module over $\mathbb{Z}$ which is a PID, Λ admits a $\mathbb{Z}$-basis whose cardinality is $4n$. Suppose that we know such a basis $(e_1, e_2, \ldots, e_{4n})$. For every $1 \leq l \leq 4n$, let us write $e_l =$

$\beta_{l,i} + \beta_{l,2}i + \beta_{l,3}j + \beta_{l,4}k$ where $\beta_{l,m} \in K$ for every m. Now, consider the matrix $M \in M_{4n}(\mathbb{R})$ defined by

$$M = \begin{pmatrix} \sigma_1(\beta_{1,1}) & \sigma_1(\beta_{2,1}) & \dots & \sigma_1(\beta_{4n,1}) \\ \sigma_2(\beta_{1,1}) & \sigma_2(\beta_{2,1}) & \dots & \sigma_2(\beta_{4n,1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta_{1,1}) & \sigma_n(\beta_{2,1}) & \dots & \sigma_n(\beta_{4n,1}) \\ \sigma_1(\beta_{1,2}) & \sigma_1(\beta_{2,2}) & \dots & \sigma_1(\beta_{4n,2}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta_{1,2}) & \sigma_n(\beta_{2,2}) & \dots & \sigma_n(\beta_{4n,2}) \\ \sigma_1(\beta_{1,3}) & \sigma_1(\beta_{2,3}) & \dots & \sigma_1(\beta_{4n,3}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta_{1,3}) & \sigma_n(\beta_{2,3}) & \dots & \sigma_n(\beta_{4n,3}) \\ \sigma_1(\beta_{1,4}) & \sigma_1(\beta_{2,4}) & \dots & \sigma_1(\beta_{4n,4}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta_{1,4}) & \sigma_n(\beta_{2,4}) & \dots & \sigma_n(\beta_{4n,4}) \end{pmatrix}.$$

Then it is not difficult to see that we have $\Phi(F) = M \cdot \mathbb{Q}^{4n}$, $\mathcal{R} = \Phi(\Lambda) = M \cdot \mathbb{Z}^{4n}$, $\mathcal{F} = M \cdot [0,1)^{4n}$, $\Delta = M \cdot (\mathbb{Q} \cap [0,1))^{4n}$ and $\overline{\mathcal{F}} = \overline{\Delta} = M \cdot [0,1]^{4n}$. Now, as in the totally real number field case (see [4]) we consider a cutting-covering of $\overline{\mathcal{F}} = \overline{\Delta}$ using parallelotopes whose faces are orthogonal to the canonical axes of $\mathbb{R}^{4n}$. These parallelotopes $\mathcal{P}$ are of the form

$$\mathcal{P} = \{(u_l)_{1 \le l \le 4n} \in \mathbb{R}^{4n};\ |u_l - C_l| \le h_l\}, \tag{15}$$

where $C = (C_l)_{1 \le l \le 4n}$ is the center of the parallelotope and $0 < h_l$ for every l. The way we obtain a cutting-covering of $\overline{\mathcal{F}}$ is similar to the way we proceed in the totally real number field case, so we refer to [4] for details. The structure of the algorithm is also the same. Let us recall its general strategy and explain where differences occur.

Assume that we have an idea of $M(\Lambda)$ denoted k. Suppose that we have at our disposal a set $\mathcal{X}$ of elements of $\mathcal{R}$, and let us take a small $\epsilon > 0$.

Definition 4.1. A subset of $\mathbb{R}^{4n}$ will be said to be *absorbed* by $X \in \mathcal{X}$, if it is contained in the region defined by the inequality $N_{\mathbb{R}}(x - X) \le k - \epsilon$.

The computations are organized as described in Algorithm 2.

4.2. **The absorption test.** Let $\mathcal{P}$ be a parallelotope defined as in (15) and X be some element of $\mathcal{R}$. Since for $t \in \mathbb{R}^{4n}$ we have

$$N_{\mathbb{R}}(t) = \prod_{i=1}^{n} (t_i^2 - \sigma_i(a) t_{i+n}^2 - \sigma_i(b) t_{i+2n}^2 + \sigma_i(ab) t_{i+3n}^2),$$

where for every i, $\sigma_(a), \sigma_i(b) < 0$, we see that $\mathcal{P}$ is absorbed by X if

$$\prod_{i=1}^{n} A_i(\mathcal{P}, X) \le k - \epsilon. \tag{16}$$

where

$$\begin{aligned} A_i(\mathcal{P}, X) \quad = \quad & \big(|C_i - X_i| + h_i\big)^2 - \sigma_i(a)\big(|C_{i+n} - X_{i+n}| + h_{i+n}\big)^2 \\ & -\sigma_i(b)\big(|C_{i+2n} - X_{i+2n}| + h_{i+2n}\big)^2 \\ & +\sigma_i(ab)\big(|C_{i+3n} - X_{i+3n}| + h_{i+3n}\big)^2. \end{aligned}$$

Algorithm 2: Computation of $M(\Lambda)$

Input: Λ, order of quaternion field F over K.
Output: $M(\Lambda)$ or *failure*.

1 Cover $\overline{\mathcal{F}}$ with parallelotopes as described above.
2 Choose $k > 0$, choose a list $\mathcal{X}$ of small elements of $\mathcal{R}$: for instance, $X \in \mathcal{X}$ iff $X = MT$ where $T \in \mathbb{Z}^{4n}$ and $-B \leq T_i \leq B + 1$ for some bound $B \geq 0$
3 *Absorption test*
Eliminate all the parallelotopes which are absorbed by elements of $\mathcal{X}$. Every parallelotope which cannot be eliminated is stored in a list of so-called *problematic parallelotopes*. Let $\mathcal{P}_i$, $i = 1 \dots N$ be this list at the end of this step. Every x in the union $\mathcal{G}$ of the parallelotopes which have been eliminated, satisfies $\tilde{m}_\Lambda(x) \leq k - \epsilon$.
4 *Units test*
Use the action of the unit group $\mathbb{Z}_K^\times$. We choose a unit $\varepsilon \neq \pm 1$. First, we eliminate every $\mathcal{P}_i$ such that $\Phi(\varepsilon) \star \mathcal{P}_i \subset \mathcal{G} + \mathcal{R}$, and enlarge $\mathcal{G}$ gradually. Then we repeat this elimination loop until the number N of remaining parallelotopes stabilizes. Of course we can use successively several units. If there remains no parallelotope, then $M(\Lambda) < k$; go back to Step 2 with a smaller value of k.
5 *Further cutting*
Cut every remaining parallelotope into 2^{4n} smaller parallelotopes, and restart the whole process from Step 3 while the number of remaining parallelotopes decreases.
6 *Analysis*
We analyze the smallest collection of problematic parallelotopes that we have obtained, thanks to Theorem 3.2. This Theorem, if it can be used, allows us to obtain a finite set $\mathcal{E}$ of potentially critical points $t_i \in \Phi(F)$. We can compute $\tilde{m}_\Lambda(t_i)$ for $t_i \in \mathcal{E}$ by Algorithm 1. With the notations of Theorem 3.2, if $m_\Lambda(G) = \max\{\tilde{m}_\Lambda(t_i);\ t_i \in \mathcal{E}\} \geq k$, we have $M(\Lambda) = \widetilde{M}(\Lambda) = m_\Lambda(G)$ and $\mathcal{E}'$ is the set of the only critical points in $\Phi(F)$ modulo $\mathcal{R}$. If we cannot apply Theorem 3.2, the algorithm returns *failure*, but we can start again with new parameters in Step 2.

Moreover, the upper bound used in (16) is optimal because there exists a vertex S of $\mathcal{P}$ which satisfies $N_{\mathbb{R}}(S - X) = \prod_{i=1}^{n} A_i(\mathcal{P}, X)$.

4.3. **The units test.** Let $\varepsilon \neq \pm 1$ be the unit of $\mathbb{Z}_K$ used for this test. Write $\{\mathcal{P}_1, \dots, \mathcal{P}_N\}$ for the set of problematic parallelotopes remaining after Step 3, and for every $p \in \{1, \dots, N\}$, let us denote by D_p the center of $\mathcal{P}_p$. Let $\mathcal{P}$ be one of these parallelotopes, centered in C: $\mathcal{P} = \{(u_l)_{1 \leq l \leq 4n} \in \mathbb{R}^{4n};\ |u_l - C_l| \leq h_l\}$. Then $\varepsilon \star \mathcal{P}$ is a parallelotope centered in C'' where $C''_{i+kn} = \sigma_i(\varepsilon) C_{i+kn}$ for $1 \leq i \leq n$ and $0 \leq k \leq 3$ and whose faces are also orthogonal to the canonical axes of $\mathbb{R}^{4n}$. More precisely

$$\varepsilon \star \mathcal{P} = \{(v_l)_{1 \leq l \leq 4n};\ |v_l - C''_l| \leq h'_l\},$$

where $h'_{i+kn} = |\sigma_i(\varepsilon)| h_{i+kn}$ for $1 \leq i \leq n$ and $0 \leq k \leq 3$. Let us put $(T_1, \dots, T_{4n}) = M^{-1}C''$, $X_0 = M(\lfloor T_1 \rfloor, \dots, \lfloor T_{4n} \rfloor) \in \mathcal{R}$ and $C' = C'' - X_0 \in \overline{\mathcal{F}}$. Let us write $M^{-1} = (m'_{i,j})_{1 \leq i,j \leq 4n}$. We first determine a list of elements of $\mathcal{R}$ containing all the $X \in \mathcal{R}$ such that $\varepsilon \star \mathcal{P} - X$ meets $\overline{\mathcal{F}}$. Using the same argument as in [4] we see that such an X is of the form

$$X = X_0 + M(\nu_1, \dots, \nu_{4n}), \tag{17}$$

where for every i, $\nu_i \in \mathbb{Z} \cap [\lfloor \alpha_i \rfloor, \lfloor \beta_i \rfloor]$, $\alpha_i = \sum_{j=1}^{4n} m'_{i,j}(C'j - \delta_{i,j}h'_j)$, $\beta_i = \sum_{j=1}^{4n} m'_{i,j}(C'j + \delta_{i,j}h'_j)$ and $\delta_{i,j} = 1$ or -1 according to whether $m'_{i,j} > 0$ or not. Remark that X_0 satisfies (17) and denote by $X_0, X_1, \ldots, X_g$ ($g \geq 0$) all the elements of $\mathcal{R}$ satisfying (17). As in [4], if for all j ($0 \leq j \leq g$) we have

$$\begin{cases} \text{for all } p \in \{1, \ldots, N\}, \text{ there exists } i_p \in \{1, \ldots n\} \text{ and } k \in \{0, \ldots, 3\} \\ \text{such that } |(C'' - X_j - D_p)_{i_p+kn}| > \left(1 + |\sigma_{i_p}(\varepsilon)|\right) h_{i_p+kn}, \end{cases}$$

then $\mathcal{P}$ can be eliminated from the list of problematic parallelotopes.

4.4. **Termination without failure.** It can be shown, using arguments similar to those that are used in [2, 8, 5] (see in particular [5, Proposition 4.25]), that the algorithm terminates as soon as $n > 2$ for a good choice of k and a sufficiently thin initial cutting-covering. But, in the case $n = 2$, which is the only case that we can treat with our computers, nothing can be said a priori.

5. The algorithm, technical aspect

5.1. **Symmetry and fundamental domain.** For any $x \in \mathbb{R}^{4n}$, we have $\tilde{m}_\Lambda(x) = \tilde{m}_\Lambda(-x)$. Therefore, we can restrict our calculation to one half of $\overline{\mathcal{F}}$ in Step 3 of Algorithm 2. Nevertheless, the symmetry should be kept in mind for the remainder of the algorithm (e.g. for Step 4, we should take it into account for $\mathcal{G}$).

Some problematic parallelotopes can lie on the boundary of the fundamental domain, which may add unnecessary vertices to the digraph, making it non convenient. To tackle this issue, we change the fundamental domain by translating the problematic parallelotopes or the fundamental domain itself (which is equivalent anyway). For more details, see [4, Section 5.7.2].

5.2. **Initial value of k.** Algorithm 2 requires an initial value of k in Step 2. For the algorithm to be successful, we need $k \leq M(\Lambda)$. If every parallelotope is eliminated by the absorption of integers or the action of units, then $M(\Lambda) < k$ and we can start again with smaller k.

We observe that the points $x \in F$ such that $M(\Lambda) = m_\Lambda(x)$ have a "small" orbit under the action of units. Therefore, if we denote by ε a unit of K which is not a root of unity, then $\varepsilon^\ell x - x \in \Lambda$ for some "small" $\ell \in \mathbb{Z}_{>0}$. In other words, there exist some $a \in \Lambda$ and some "small" $\ell \in \mathbb{Z}_{>0}$ such that

$$x = \frac{a}{\varepsilon^\ell - 1}.$$

We may study such points and apply Algorithm 1 to find their minimum $m_\Lambda(x)$. This can provide a lower bound on $M(\Lambda)$.

This heuristic can turn out to be non applicable when $N_{K/\mathbb{Q}}(\varepsilon^\ell - 1)$ is large. Instead, we can simply consider points

$$x = \frac{a}{b},$$

where b is a factor of $\varepsilon^\ell - 1$ of small norm.

5.3. **Analysis of the digraph.** In Step 6 of Algorithm 2, we try to apply Theorem 3.2, that is to say to obtain a convenient graph. This digraph may be not convenient, but we can try to simplify it to make it convenient, as in [11, Section 3.2.2]. The basic idea is to merge parallelotopes which have the same translation vector. For example, in Figure 1c, we can merge $\mathcal{T}_1$, $\mathcal{T}_2$, and $\mathcal{T}_3$ to make the digraph convenient.

5.4. **Execution of Algorithm 1.** Once we have a convenient digraph, it remains to apply Algorithm 1 to a finite set of points. This algorithm is described with elements of $\mathbb{R}^{4n}$, which would suggest using floating point numbers, but it actually deals with elements of F. Consequently, the orbit is computed as a subset of the quaternion field F in Step 1.

In practice, we compute the orbit of $x = \Phi(\xi) \in \Phi(F)$, where $\xi \in F$ as follows. Let $\{\varepsilon_i,\, 1 \leq i < n\}$ be a fundamental system of units of K. For fixed $1 \leq i < n$ and for increasing $k \geq 1$, we compute the elements $\varepsilon_i^k \cdot \xi$ reduced modulo Λ, which is denoted by $\overline{\varepsilon_i^k \cdot \xi}^{red}$, until $\overline{\varepsilon_i^k \cdot \xi}^{red} = \overline{\xi}^{red}$, which happens for some finite $m_i \geq 1$. Then the orbit of x is the image by Φ of the set

$$\left\{ \overline{\pm \prod_{i=1}^{n-1} \overline{\varepsilon_i^{k_i} \cdot \xi}^{red}}^{red} \;,\; 0 \leq k_j < m_j \text{ for any } 1 \leq j < n \right\},$$

where repetitions are discarded.

As for Steps 2 and 6, to compute $\mathcal{M}_{k'}$ or $\mathcal{M}_k$, we deal with quantities $N_{\mathbb{R}}(z - Z)$ (see (1)) which are in fact rational numbers.Therefore, during the actual execution of the algorithm we can compute exactly these numbers and the output of Algorithm 2 is a rational number (whenever its execution is successful).

6. Results

6.1. **An example.** Let us introduce this section with an example. We know by [2] that if $K = \mathbb{Q}(\sqrt{2})$, $F = \left(\dfrac{-1,-1}{K}\right)$ and Λ is a maximal order of F, then $M(\Lambda) \leq \frac{1}{2}$. Let us consider the maximal order

$$\Lambda = \mathbb{Z}_K \oplus \mathbb{Z}_K \frac{\sqrt{2}(1+i)}{2} \oplus \mathbb{Z}_K \frac{\sqrt{2}(1+j)}{2} \oplus \mathbb{Z}_K \frac{1+i+j+k}{2}.$$

Since there exist elements $\lambda \in \Lambda$ satisfying $N(\lambda) = 2$ which implies $m_\Lambda(\frac{1}{\lambda}) = \frac{1}{2}$, we know that $M(\Lambda) \geq \frac{1}{2}$. Consequently we have

$$M(\Lambda) = \frac{1}{2}.$$

Now, let us come back to our algorithm. A $\mathbb{Z}$-basis of Λ is for instance

$$\left(1, \sqrt{2}, \frac{\sqrt{2}}{2}(1+i), 1+i, \frac{\sqrt{2}}{2}(1+j), 1+j, \frac{1}{2}(1+i+j+k), \frac{\sqrt{2}}{2}(1+i+j+k)\right)$$

and, according to this choice of basis, the matrix of the fundamental embedding is

$$M = \begin{pmatrix}
1 & \sqrt{2} & \sqrt{2}/2 & 1 & \sqrt{2}/2 & 1 & 1/2 & \sqrt{2}/2 \\
1 & -\sqrt{2} & -\sqrt{2}/2 & 1 & -\sqrt{2}/2 & 1 & 1/2 & -\sqrt{2}/2 \\
0 & 0 & \sqrt{2}/2 & 1 & 0 & 0 & 1/2 & \sqrt{2}/2 \\
0 & 0 & -\sqrt{2}/2 & 1 & 0 & 0 & 1/2 & -\sqrt{2}/2 \\
0 & 0 & 0 & 0 & \sqrt{2}/2 & 1 & 1/2 & \sqrt{2}/2 \\
0 & 0 & 0 & 0 & -\sqrt{2}/2 & 1 & 1/2 & -\sqrt{2}/2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1/2 & \sqrt{2}/2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1/2 & -\sqrt{2}/2
\end{pmatrix}.$$

We use the following cutting-covering of $\overline{\mathcal{F}}$: if $a_l = \min\{x_l;\, x \in \overline{\mathcal{F}}\}$ and $b_l = \max\{x_l;\, x \in \overline{\mathcal{F}}\}$ for every $1 \leq l \leq 8$, we put $h_l = (b_l - a_l)/2n_l$ where $n_1 = n_2 = 70$, $n_3 = n_4 = n_5 = n_6 = 30$, $n_7 = n_8 = 12$ and we cover $\overline{\mathcal{F}}$ with parallelotopes $\mathcal{P}$ as in (15) where for every l, $C_l = a_l + (2i_l + 1)h_l$ for some $0 \leq i_l \leq n_l - 1$. Of course, as in the number field case, we only consider parallelotopes that intersect $\overline{\mathcal{F}}$. Running Algorithm 2 with $k = 1/2$, $\mathcal{X} = M \cdot ([-2, 3] \cap \mathbb{Z})^8$, after four loops of Steps 3, 4,

and 5, we finally obtain a convenient digraph composed of nine disjointed simple circuits whose length is 1. This leads to $\mathcal{E} = \{t_i = \Phi(\xi_i);\ 1 \le i \le 9\}$ where

- $\xi_1 = \frac{2+3\sqrt{2}}{4} + \frac{\sqrt{2}}{4}i + \frac{2+\sqrt{2}}{4}j + \frac{\sqrt{2}}{4}k$;
- $\xi_2 = \frac{2+\sqrt{2}}{4} + \frac{\sqrt{2}}{4}i + \frac{2+\sqrt{2}}{4}j + \frac{\sqrt{2}}{4}k$;
- $\xi_3 = \frac{1+\sqrt{2}}{2} + \frac{1}{2}j$;
- $\xi_4 = \frac{2+3\sqrt{2}}{4} + \frac{2+\sqrt{2}}{4}i + \frac{\sqrt{2}}{4}j + \frac{\sqrt{2}}{4}k$;
- $\xi_5 = \frac{4+3\sqrt{2}}{4} + \frac{2+\sqrt{2}}{4}i + \frac{2+\sqrt{2}}{4}j + \frac{\sqrt{2}}{4}k$;
- $\xi_6 = \frac{2+\sqrt{2}}{4} + \frac{2+\sqrt{2}}{4}i + \frac{\sqrt{2}}{4}j + \frac{\sqrt{2}}{4}k$;
- $\xi_7 = \frac{4+\sqrt{2}}{4} + \frac{2+\sqrt{2}}{4}i + \frac{2+\sqrt{2}}{4}j + \frac{\sqrt{2}}{4}k$;
- $\xi_8 = \frac{1+\sqrt{2}}{2} + \frac{1}{2}i$;
- $\xi_9 = \frac{2+\sqrt{2}}{2} + \frac{1}{2}i + \frac{1}{2}j$.

Algorithm 1 gives $\tilde{m}_\Lambda(t_i) = 1/2$ for every $1 \le i \le 9$ so that $M(\Lambda) = \widetilde{M}(\Lambda) = 1/2$. In fact, we do not have to compute these minima because for every $1 \le i \le 9$ we have $x_i \equiv 1/X_i \bmod \Lambda$ where $N(X_i) = 2$. For instance we can take

- $X_1 = \frac{1+\sqrt{2}}{2} + \frac{1}{2}i + \frac{1+\sqrt{2}}{2}j + \frac{1}{2}k$;
- $X_2 = \frac{1+\sqrt{2}}{2} - \frac{1}{2}i + \frac{1+\sqrt{2}}{2}j + \frac{1}{2}k$;
- $X_3 = \frac{2+\sqrt{2}}{2} + \frac{\sqrt{2}}{2}j$;
- $X_4 = \frac{1+\sqrt{2}}{2} + \frac{1+\sqrt{2}}{2}i + \frac{1}{2}j + \frac{1}{2}k$;
- $X_5 = -\frac{1}{2} - \frac{1+\sqrt{2}}{2}i + \frac{1+\sqrt{2}}{2}j + \frac{1}{2}k$;
- $X_6 = \frac{1}{2} - \frac{1}{2}i + \frac{1+\sqrt{2}}{2}j + \frac{1+\sqrt{2}}{2}k$;
- $X_7 = \frac{1}{2} - \frac{1+\sqrt{2}}{2}i + \frac{1+\sqrt{2}}{2}j + \frac{1}{2}k$;
- $X_8 = \frac{2+\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$;
- $X_9 = \frac{-2+\sqrt{2}}{2}i + \frac{\sqrt{2}}{2}j$.

This leads to $M(\Lambda) = 1/2$ as expected.

Of course, and this is the interest of the algorithm, in general we do not have any theoretic argument that allows to establish the value of $M(\Lambda)$ as in the previous example.

6.2. **Some other results.** Table 1 gives some of the results that we have obtained. More extensive tables are available from [7]. In this table, K is a number field, F is a quaternion field and Λ is an order of F. For brevity, the order Λ is described by a quadruple $(q_1, q_2, q_3, q_4) \in F^4$ such that $\Lambda = \oplus_{i=1}^4 q_i \mathbb{Z}_K$, which is always possible in the cases that we have studied. The column *Max* indicates if Λ is maximal or not (maximal orders were obtained with [3]), T is the number of critical points in $\Phi(F)$ modulo $\mathcal{R} = \Phi(\Lambda)$ and $M(\Lambda)$ is the Euclidean minimum of Λ.

6.3. **Timings.** The time required to execute Algorithm 2 obviously depends on the choice of parameters. Indeed, if we choose $k > 0$ strictly larger than $M(\Lambda)$, then we will have to start again with a smaller value of k. The timings presented here are for a choice of k smaller than $M(K)$, typically $k = M(\Lambda) - \epsilon$, where $\epsilon = 10^{-4}$.

In Table 2, the orders are the maximal orders corresponding to the quaternion field given in Table 1. It should be noted that no particular efficiency was pursued for Step 6 because it turned out to be short enough in the examples considered.

The times given are total computation times (cpu times). The computations were carried out on an Intel Xeon E5-2680 (2.50GHz) processor with 24 cores.

d	F	Λ	Max	T	$M(\Lambda)$
$\mathbb{Q}(\sqrt{2})$	$\left(\frac{-1,-1}{K}\right)$	$\left(1, \frac{\sqrt{2}(1+i)}{2}, \frac{\sqrt{2}(1+j)}{2}, \frac{1+i+j+k}{2}\right)$	yes	9	1/2
	$\left(\frac{-1,-1}{K}\right)$	$(1,i,j,k)$	no	1	4
	$\left(\frac{-3,-\sqrt{2}-2}{K}\right)$	$\left(1, \frac{1+i}{2}, j, \frac{j+k}{2}\right)$	yes	36	$\frac{41}{16}$
$\mathbb{Q}(\sqrt{3})$	$\left(\frac{-1,-1}{K}\right)$	$\left(1, \frac{1+i}{2}(\sqrt{3}+1), \frac{1+j}{2}(\sqrt{3}+1), \frac{1+i+j+k}{2}\right)$	yes	9	1
	$\left(\frac{-1,-1}{K}\right)$	$\left(1, i, \frac{\sqrt{3}+j}{2}, \frac{\sqrt{3}i-k}{2}\right)$	yes	9	1
$\mathbb{Q}(\sqrt{5})$	$\left(\frac{-1,-1}{K}\right)$	$\left(1, i, \frac{1+\sqrt{5}+(3+\sqrt{5})i+2j}{4}, \frac{1+i+j+k}{2}\right)$	yes	3	1/4
	$\left(\frac{-1,\sqrt{5}-7}{K}\right)$	$\left(1, i, \frac{\sqrt{5}+3}{4}(1+i) + \frac{j}{2}, \frac{\sqrt{5}+3}{4} + \frac{k}{2}\right)$	yes	6	9/4
$\mathbb{Q}(\sqrt{13})$	$\left(\frac{-1,-1}{K}\right)$	$\left(1, i, \frac{3+\sqrt{13}}{4} + \frac{(5+\sqrt{13})i}{4} + \frac{j}{2}, \frac{1+i+j+k}{2}\right)$	yes	24	3/4

TABLE 1. Euclidean minima of some quaternion fields.

F	time for loops of absorption and units (Steps 3 to 5)	time for tests (Step 6)	total time
$\left(\frac{-1,-1}{\mathbb{Q}(\sqrt{2})}\right)$	24h16min	44min	25h2min
$\left(\frac{-1,-\sqrt{5}-7}{\mathbb{Q}(\sqrt{5})}\right)$	7h19min	5 min	7h25min
$\left(\frac{-1,-1}{\mathbb{Q}(\sqrt{13})}\right)$	9d12h36min	1d2h41min	10d15h21min

TABLE 2. Some timings for Algorithm 2.

ACKNOWLEDGMENTS

The research of the second author was funded by a "nouveau chercheur" grant by région Auvergne. Parts of this research were conducted during a visit of the second author to Bordeaux, funded by ERC Starting Grant ANTICS 278537. Both authors would like to thank the anonymous reviewer for her/his remarks and corrections.

Experiments presented in this paper were carried out using the PLAFRIM experimental testbed, being developed under the Inria PlaFRIM development action with support from Bordeaux INP, LABRI and IMB and other entities: Conseil Régional d'Aquitaine, Université de Bordeaux and CNRS, and ANR in accordance to the "programme d'investissements d'Avenir" (see `http://www.plafrim.fr`).

References

[1] E.S. Barnes, H.P.F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms (II), *Acta Mathematica* **88** (1952), 279–315

[2] E. Bayer, J.-P. Cerri, J. Chaubert, Euclidean minima and central division algebras, *International Journal of Number Theory* **5** (2009), 1155–1168

[3] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.20-5 (2016), `http://magma.maths.usyd.edu.au/magma/`

[4] J.-P. Cerri, Euclidean minima of totally real number fields: Algorithmic determination, *Mathematics of Computation* **76** (2007), 1547–1575

[5] J.-P. Cerri, Spectres euclidiens et inhomogènes des corps de nombres, *Thèse de Doctorat, Université Henri Poincaré, Nancy* (2005) available from `https://hal.archives-ouvertes.fr/tel-00011151`

[6] J.-P. Cerri, J. Chaubert, P. Lezowski, Euclidean totally definite quaternion fields over the rational field and over quadratic number fields, *International Journal of Number Theory*, **9**, 3 (2013), 653–673

[7] J.-P. Cerri, P. Lezowski, Tables of Euclidean minima of orders in totally definite quaternion fields over quadratic fields, `http://www.math.u-bordeaux.fr/~jcerri/articles/table_quaternions.php`

[8] J. Chaubert, Minimum euclidien des ordres maximaux dans les algèbres centrales à division, PhD Thesis, EPFL (2006)

[9] M. Deuring, Algebren, Springer Verlag, New-York (1968)

[10] M. Dutour Sikirić, A. Schürmann and F. Vallentin, Complexity and algorithms for computing Voronoi cells of lattices, *Mathematics of Computation* **78** (2009), 1713–1731.

[11] P. Lezowski, Computation of the Euclidean Minimum of Algebraic Number Fields, *Mathematics of Computation* **83** (2014), 1397–1426

[12] The PARI Group, PARI/GP version `2.9.0`, Univ. Bordeaux, 2016, `http://pari.math.u-bordeaux.fr/`

[13] I. Reiner, Maximal orders, Clarendon Press, Oxford, 2003

[14] A. Schürmann, Computational Geometry of Positive Definite Quadratic Forms (chapter 4), *University Lecture Series*, AMS, Providence, RI, 2009.

[15] M.-F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Math. 800, Springer, Berlin, 1980

IMB, Université de Bordeaux, 351, cours de la Libération, 33400 Talence, France
E-mail address: `jean-paul.cerri@math.u-bordeaux.fr`

Université Clermont Auvergne, Laboratoire de Mathématiques Blaise Pascal,, F-63000 Clermont-Ferrand
E-mail address: `pierre.lezowski@math.univ-bpclermont.fr`